

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-008619

(43)Date of publication of application : 12.01.1999

(51)Int.Cl.

H04L 9/32

G09C 1/00

H04L 9/08

(21)Application number : 09-160798

(71)Applicant : HITACHI LTD

(22)Date of filing : 18.06.1997

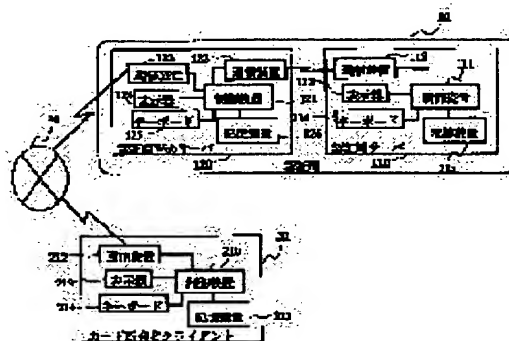
(72)Inventor : TOMIYAMA TOMOYA
CHIBA SANEYUKI
KAWATSURE YOSHIKI
MATSUNAGA KAZUO
SUZAKI SEIICHI

(54) ELECTRONIC CERTIFICATE PUBLICATION METHOD AND SYSTEM THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To issue a certificate at a low cost and to enhance the security at the issue.

SOLUTION: In the electronic certificate publication method, an authentication station issues an electronic certificate via a network to a person to be authenticated who receives an issued certificate. The authentication station receives a document to be certificated in which a digital signature is made by using a key certificated by an electronic certificate and the name of the document to be certificated on request of issue from a client 20 based on the electronic certificate of a public key having already been issued by an authentication station 10 and on a public key of the person to be authenticated in the electronic certificate to authenticate whether or not the digital signature by the person to be authenticated is valid. When the digital signature is authenticated to be valid, the document is collated with a list containing electronic certificates to be issued. In the case that the certificate requested by the authenticated person is able to be issued, the sent electronic certificate is authenticated, and when the authentication of the certificate is valid, the electronic certificate authenticating the public key of the authenticated person is issued.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

BEST AVAILABLE COPY

[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision
of rejection]
[Date of requesting appeal against examiner's
decision of rejection]
[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-8619

(43) 公開日 平成11年(1999) 1月12日

(51) Int.Cl. ⁸	識別記号	F I
H 0 4 L 9/32		H 0 4 L 9/00 6 7 5 D
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00 6 6 0 B
H 0 4 L 9/08		H 0 4 L 9/00 6 0 1 F

審査請求 未請求 請求項の数 5 O L (全 16 頁)

(21) 出願番号 特願平9-160798

(22) 出願日 平成9年(1997) 6月18日

(71) 出願人 000005108

株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地

(72) 発明者 富山 朋哉

神奈川県横浜市都筑区加賀原二丁目2番
株式会社日立製作所ビジネスシステム開発
センタ内

(72) 発明者 千葉 實之

神奈川県横浜市都筑区加賀原二丁目2番
株式会社日立製作所ビジネスシステム開発
センタ内

(74) 代理人 弁理士 秋田 収喜

最終頁に続く

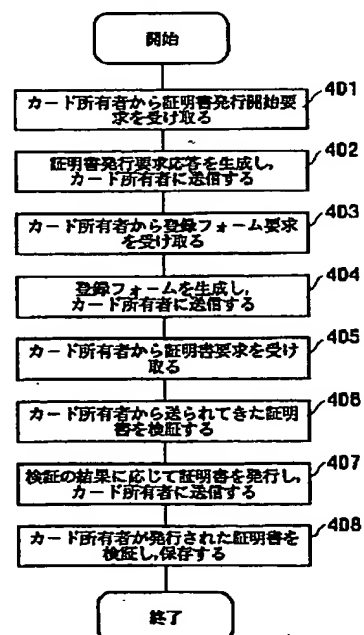
(54) 【発明の名称】 電子証明書発行方法及びシステム

(57) 【要約】

【課題】 低コストで証明書を発行することとその発行の際のセキュリティ強度を高めること。

【解決手段】 証明書を発行してもらう被認証者に対して認証局がネットワークを介して電子証明書を発行する電子証明書発行方法であって、ある認証局が既に発行した公開鍵の電子証明書とその電子証明書における被認証者の公開鍵に対して、前記電子証明書で証明済の鍵でデジタル署名を施したものと発行を要求する証明書名の入力を受け、前記被認証者のデジタル署名が妥当であるか否かを検証し、妥当であると検証できたときは、前記電子証明書で発行可能な証明書のリストと照合し、前記被認証者が要求した証明書が発行可能である場合には、送信された電子証明書の検証を行い、検証できた場合に、前記被認証者の公開鍵を認証した電子証明書を発行する。

図4



【特許請求の範囲】

【請求項 1】 証明書を発行してもらう被認証者に対して認証局がネットワークを介して電子証明書を発行する電子証明書発行方法であって、

ある認証局が既に発行した公開鍵の電子証明書とその電子証明書における被認証者の公開鍵に対して、前記電子証明書で証明済の鍵でデジタル署名を施したものと発行を要求する証明書名の入力を受け、前記被認証者のデジタル署名が妥当であるか否かを検証し、妥当であると検証できたときは、前記電子証明書で発行可能な証明書のリストと照合し、前記被認証者が要求した証明書が発行可能である場合には、送信された電子証明書の検証を行い、検証できた場合に、前記被認証者の公開鍵を認証した電子証明書を発行することを特徴とする証明書発行方法。

【請求項 2】 前記請求項 1 に記載の電子証明書発行方法であって、

前記ある認証局が既に発行した公開鍵の電子証明書とその電子証明書における被認証者の公開鍵と発行を要求する証明書名と共に予め認証局に登録してある被認証者を特定する確認情報を前記電子証明書で証明済の鍵でデジタル署名を施したものの入力を受け、前記被認証者のデジタル署名が妥当であるか否かを検証し、妥当であると検証できた後に、前記被認証者の確認情報の検証を行い、検証できたときに前記電子証明書で発行可能な証明書のリストと照合することを特徴とする証明書発行方法。

【請求項 3】 電子証明書を発行してもらう被認証者のクライアントと、前記被認証者に電子証明書を発行する認証局のサーバとがネットワークを介して接続されてなる電子証明書発行システムであって、前記被認証者のクライアントは、ある認証局が既に発行した公開鍵の電子証明書とその電子証明書における被認証者の公開鍵に対し、前記電子証明書で証明済の鍵でデジタル署名し、前記認証局のサーバに送信して他の電子証明書の発行要求を行う発行要求手段と、前記認証局から送信されてきた電子証明書を保存する手段とを備え、前記認証局のサーバは、各電子証明書から発行可能な他の電子証明書群をまとめた発行可能証明書リストと、前記被認証者のデジタル署名が妥当であるか否かを検証する署名検証手段と、前記署名検証手段により、署名が妥当であると検証できたときに、送信されてきた送信電子証明書と発行可能証明書リストと照合する証明書照合手段と、前記証明書照合手段により、前記被認証者が要求した要求電子証明書が発行可能であるとき、前記被認証者からの送信電子証明書の検証を行う電子証明書検証手段と、前記電子証明書検証手段により、前記送信電子証明書が検証されたとき、前記被認証者の公開鍵を認証した要求電子証明書を発行する手段とを備えたことを特徴とする電子証明書発行システム。

【請求項 4】 前記請求項 3 に記載の電子証明書発行システムにおいて、

前記被認証者のクライアントの発行要求手段は、予め認証局に登録してある被認証者を特定する確認情報を前記電子証明書で証明済の鍵でデジタル署名したものを送信する手段を備え、

前記認証局のサーバは、前記被認証者の確認情報の検証を行う確認情報検証手段を備えたことを特徴とする電子証明書発行システム。

【請求項 5】 前記請求項 3、または 4 に記載の電子証明書発行システムにおいて、

前記認証局のサーバは、前記発行可能証明書リストを基に、送信電子証明書で発行可能な他の電子証明書のリスト、または前記要求電子証明書の発行に必要な電子証明書を前記被認証者のクライアントに送信する手段を備えたことを特徴とする電子証明書発行システム。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、公開鍵暗号方式を用いたオープンなネットワーク上で行われる電子証明書発行およびシステムに関し、特に低コストで証明書を発行できる電子証明書発行方法およびシステムに適用して有効な技術に関するものである。

【0002】

【従来の技術】 近年では、インターネットなどオープンなネットワーク上で電子商取引が行われているが、インターネットを用いて電子商取引を行う場合には個人情報等のデータのやり取りの安全性が問題となっている。

【0003】 つまり、データの漏洩や、改竄、配送元のなりすまし等の犯罪を比較的容易に行うことができるからである。

【0004】 このような問題に対して、従来では、共通鍵暗号方式や、公開鍵暗号方式といった暗号化方式を使って、安全なデータのやり取りが実現されている。

【0005】 ここで、共通鍵暗号方式とは、暗号化する時に使用する鍵と復号化する時に使用する鍵が同じである暗号方式であり、暗・復号速度が高速なので、大量のデータを暗号化するのに適している。

【0006】 これに対して公開鍵暗号方式とは、他者に見せない鍵（秘密鍵）と、それに対応する、他者に公開する鍵（公開鍵）とのペアからなり、一方の鍵を使用して作られた暗号文は、ペアのもう一方の鍵を使用しなければ復号化できない方式であり、また、一方の鍵からもう片方の鍵を類推することは困難であるという性質をっており、不特定多数の人と通信することに適している。

【0007】 また、これらの他にも認証局という、信頼できる第三者機関が発行した電子証明書（以下、証明書と記す）を使用することにより、通信相手の身元を証明し、通信元のなりすましを防止する方法が提案されてい

る。

【0008】この認証局が証明書を発行する手順は、次の通りである。

【0009】まず、被認証者が認証局に対して発行要求メッセージを送り、認証局から認証局の証明書入手する。認証局の証明書を受理した被認証者は、証明書を検証する。その証明書が、上位認証局により発行されている場合、その上位認証局の証明書入手することを繰り返す。最終的に信用できる最上位の認証局の証明書を検証することにより判断する。検証できたときは、認証局に対して、発行の申請を行う証明書の種類がわかるような情報および登録フォーム要求メッセージを送る。ここで、登録フォームとは、証明書発行に必要な事柄を記入するフォームである。

【0010】このメッセージを受理した認証局は、証明書の種類を確定しその証明書発行に必要な項目を記入する登録フォームにデジタル署名をつけて被認証者に送る。

【0011】ここで、デジタル署名とは、具体的には、署名したいメッセージをハッシュ関数とよばれる特殊な関数を用いて、一定の長さのハッシュ値とよばれる値に変換したものを作成し、そのハッシュ値に対してメッセージ作成者の秘密鍵で暗号化することである。ハッシュ値は一意に定まるため、受け取ったメッセージのハッシュと、受け取ったデジタル署名を公開鍵で復号化したものが一致するかどうかを確認することにより、メッセージの改竄を確認することができる。

【0012】デジタル署名つき登録フォームを受け取った被認証者は、署名を確認し、確認できたとき、被認証者の登録鍵、すなわち公開鍵と秘密鍵を生成し、公開鍵と登録者本人であることの根拠となる個人情報、たとえば口座番号とを暗号化して認証局に送る。

【0013】認証局は、送られてきたメッセージを復号化して、登録者本人であることの根拠となる個人情報を、その情報に関する機関に問い合わせることによって確認する。例えば、個人情報として口座番号を用いた場合は、銀行に問い合わせることになる。問い合わせた結果、情報が正しいならば、被認証者の公開鍵の証明書を作成し、この証明書を被認証者へ送る。

【0014】以上のような手順は、例えば、SET(Secure Electronic Transaction Specification, Draft for testing, June 17, 1996, MasterCard, VISA)で用いられている。

【0015】

【発明が解決しようとする課題】本発明者は、上記従来技術を検討した結果、以下の問題点を見いだした。

【0016】証明書発行の際に登録者本人であることを確認する従来の方法は、被認証者から認証局へ口座番号を送り、認証局がその口座番号が正しいかどうかを銀行に確認することによって行われている。

【0017】この方法では、証明書発行の際に口座番号の確認を認証局とは別の機関(銀行)に依頼しているため、コストが大きくなるという問題点がある。

【0018】また、暗号化されているとはいえ、証明書とは直接関係のない個人情報、オープンなネットワーク上を通過するという問題点もある。

【0019】本発明の目的は、被認証者が既に取得している証明書を本人認証の根拠とすることにより、本人認証のコストを下げ、証明書発行にかかるコストを下げるのが可能な技術を提供することにある。

【0020】本発明の他の目的は、証明書発行依頼の際に、既に発行されている証明書を基に個人情報(例えば、口座番号)というプライバシーおよびセキュリティ上に問題のある情報を送信せずに済ませることにより、全体のセキュリティ強度を高めるのが可能な技術を提供することにある。

【0021】本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述及び添付図面によって明らかになるであろう。

【0022】

【課題を解決するための手段】本願において開示される発明のうち、代表的なものの概要を簡単に説明すれば、下記のとおりである。

【0023】証明書を発行してもらう被認証者に対して認証局がネットワークを介して電子証明書を発行する電子証明書発行方法であって、ある認証局が既に発行した公開鍵の電子証明書とその電子証明書における被認証者の公開鍵に対して、前記電子証明書で証明済の鍵でデジタル署名を施したものと発行を要求する証明書の入力を受け、前記被認証者のデジタル署名が妥当であるか否かを検証し、妥当であると検証できたときは、前記電子証明書で発行可能な証明書のリストと照合し、前記被認証者が要求した証明書が発行可能である場合には、送信された電子証明書の検証を行い、検証できた場合に、前記被認証者の公開鍵を認証した電子証明書を発行する。

【0024】また、電子証明書を発行してもらう被認証者のクライアントと、前記被認証者に電子証明書を発行する認証局のサーバとがネットワークを介して接続されてなる電子証明書発行システムであって、前記被認証者のクライアントは、ある認証局が既に発行した公開鍵の電子証明書とその電子証明書における被認証者の公開鍵に対し、前記電子証明書で証明済の鍵でデジタル署名し、前記認証局のサーバに送信して他の電子証明書の発行要求を行う発行要求手段と、前記認証局から送信されてきた電子証明書を保存する手段とを備え、前記認証局のサーバは、各電子証明書から発行可能な他の電子証明書群をまとめた発行可能証明書リストと、前記被認証者のデジタル署名が妥当であるか否かを検証する署名検証手段と、前記署名検証手段により、署名が妥当であると検証できたときに、送信されてきた送信電子証明書と発

行可能証明書リストと照合する証明書照合手段と、前記証明書照合手段により、前記被認証者が要求した要求電子証明書が発行可能であるとき、前記被認証者からの送信電子証明書の検証を行う電子証明書検証手段と、前記電子証明書検証手段により、前記送信電子証明書が検証されたとき、前記被認証者の公開鍵を認証した要求電子証明書を発行する手段とを備える。

【0025】

【発明の実施の形態】以下、本発明の実施の形態を図面を用いて説明する。

【0026】図1は、本発明の一実施形態にかかる証明書発行システムの構成を示すブロック図である。本実施形態では、既に取得してあるクレジットカードを基に新たな電子証明書を取得する場合を例に取り挙げて説明していく。

【0027】本実施形態の証明書発行システムは、図1に示すように、電子証明書（以下、証明書と略す）を発行する認証局10と、証明書発行を依頼する被認証者（以下、カード所有者と記す）のクライアント20と、電子商取引を行うネットワークであるインターネット30とから構成される。

【0028】上述した認証局10は、実際の処理を行う認証局サーバ110と、カード所有者のクライアント20からインターネット30経由で入力を受け付け、認証局サーバ110へ中継し、その結果を認証局サーバ110からカード所有者のクライアント20へ送信する認証局Webサーバ120とから構成される。

【0029】認証局サーバ110は、認証局Webサーバ120と通信を行う通信装置112と、表示器113と、キーボード114と、証明書データベース、証明書名データベース、認証局の署名鍵および交換鍵が格納される記憶装置115と、これら全てを制御する制御装置111とからなる。

【0030】認証局Webサーバ120は、認証局サーバ110と通信を行う通信装置122と、インターネットに接続される通信装置123と、表示器124と、キーボード125と、Webサーバソフトウェアが格納される記憶装置126と、これら全てを制御する制御装置121とからなる。

【0031】カード所有者のクライアント20では、証明書データベースやカードホルダの署名鍵、共通鍵などを格納する記憶装置211と、インターネットに接続する通信装置212と、表示器213と、キーボード214と、これら全てを制御する制御装置210とからなる。

【0032】図2は、認証局10の構成を詳細に説明するための図である。

【0033】図2に示すように、認証局10の認証局サーバ110の記憶装置115には、証明書データベース11540と証明書名データベース11530、署名鍵

公開鍵PBCPSG(11511)と署名鍵個人鍵PVCPSG(11512)とその証明書11513とからなる認証局の署名鍵11510、鍵交換鍵公開鍵PBCPEX(11521)と鍵交換鍵個人鍵PVCPEX(11522)とその証明書11523とからなる鍵交換鍵11520が保存されている。

【0034】この証明書データベース11540は、公開鍵11543と、その公開鍵の対象（持ち主）11542、証明書11541をレコードとするデータベースであり、証明書名データベース11530は、証明書名11532と、その証明書を発行するのに必要となる条件である証明書名組11533と、その証明書を使用するブランド11531をレコードとするデータベースである。

【0035】制御装置111は、通信装置112を通じて認証局Webサーバ120に接続され、必要に応じて証明書データベース11540に格納されている証明書11541、および証明書名データベース11530に格納されている証明書名組11533、認証局10の署名鍵公開鍵11511および署名鍵個人鍵11512を認証局Webサーバ120へ送信する。

【0036】認証局Webサーバ120の制御装置121は、認証局Webサーバ120のWebサーバソフトウェア12610を記憶装置126からロードし、実行する。

【0037】Webサーバソフトウェア12610は、http(Hypertext Transport Protocol)に基づいて通信を行うプログラムである。

【0038】図3は、カード所有者のクライアント20を詳細に説明するための図である。

【0039】カード所有者20のクライアントの記憶装置211には、Webブラウザソフトウェア21110と、署名鍵秘密鍵21160と、証明書データベース21140と、カード所有者20の署名鍵公開鍵PBCPSG'(21120)および署名鍵個人鍵PVCPSG'(21130)と、それぞれの共通鍵#1～#3(21171～21173)と、署名鍵公開鍵リスト21180とが保存される。

【0040】証明書データベース21150は、署名鍵公開鍵名21153、その証明書が使える相手（ブランド名）21152、証明書21151をレコードとするデータベースである。

【0041】次に、図4を用いて本実施形態の証明書発行システムの各制御装置における証明書発行処理の概要の説明を行い、その後、各ステップの詳細をそれぞれの図を用いて説明する。

【0042】カード所有者が、Webブラウザソフトウェア21110を通じて、認証局10に対して、証明書発行を依頼する（ステップ401）。

【0043】認証局10は、カード所有者のクライアン

ト20から証明書発行依頼を受け取ると、証明書発行要求応答を生成してカード所有者のクライアント20に送信する。このとき、カード所有者へ認証局の公開鍵を送付する(ステップ402)。

【0044】カード所有者は、認証局10から証明書発行要求応答を受け取り、認証局10の証明書の検証を行い、登録フォーム要求を認証局10へ送信する(ステップ403)。

【0045】認証局10は、カード所有者のクライアント20から登録フォーム要求を受け取ると、登録フォームを生成し、カード所有者のクライアント20に送信する(ステップ404)。

【0046】カード所有者は、登録フォームに必要な事項を記入し、証明書要求を認証局10へ送付する。このとき、カード所有者は、カード所有者の公開鍵を送付する(ステップ405)。

【0047】認証局10は、カード所有者のクライアント20から送られてきた登録フォームに含まれている証明書を検証する(ステップ406)。

【0048】認証局10は、ステップ406の検証結果に応じて、証明書を発行し、カード所有者のクライアント20に送付する(ステップ407)。

【0049】カード所有者のクライアント20では、発行された証明書を検証し、保存する(ステップ408)。

【0050】上述したステップ402の詳細を図5を用いて説明する。

【0051】ステップ402は、まず、認証局サーバ10が、証明書発行申請メッセージに対する応答メッセージを生成し、署名する(ステップ501)。

【0052】認証局10は、認証局10の鍵交換鍵及び署名鍵のそれぞれの公開鍵PBCPEX(11521)、PBCPSG(11511)と、それぞれの証明書CertPBCPEX(11523)、CertPBCPSG(11513)と、ステップ501で作成した署名つき応答メッセージを、カード所有者のクライアント20に送信する(ステップ502)。

【0053】次に、上述したステップ403を図6を用いて詳細に説明する。

【0054】ステップ403は、まず、カード所有者のクライアント20が、証明書CertPBCPEX(11523)、CertPBCPSG(11513)の妥当性を、SET(Secure Electronic Transaction Specification, Draft for testing, June 17, 1996, MasterCard, VISA, Book II, Part II Certificate Management, Ch.1, Sec.3, Certificate Chain Validation)と同様に検証する(ステップ601)。この妥当性の検証は、例えば、証明書が有効期限内であるか否かのチェック等である。

【0055】検証の結果、妥当でなければ処理を中断し、妥当であれば処理を続ける(ステップ602)。

【0056】カード所有者は、キーボード214を通じ

て登録フォーム選択情報を取り込む(ステップ603)。ここで、登録フォーム選択情報とは、消費者が発行してもらいたい証明書を選択するために必要な情報である。例えば、その証明書が利用できるカード会社名(ブランド名)などである。

【0057】カード所有者のクライアント20は、登録フォーム要求メッセージおよび共通鍵(#1)SymK#1を作成する(ステップ604)。

【0058】カード所有者のクライアント20は、登録フォーム要求メッセージを共通鍵SymK #1で暗号化し、また、登録フォーム選択情報と共通鍵SymK #1を認証局の鍵交換鍵公開鍵PBCPEX(11521)で暗号化する(ステップ605)。

【0059】カード所有者20は、ステップ605で作成したメッセージを認証局10へ送信する(ステップ606)。

【0060】次に、上述したステップ404を図7を用いて詳細に説明する。

【0061】ステップ404は、まず、認証局10が、認証局10の鍵交換鍵個人鍵PVCPEX1(1522)で、登録フォーム選択情報と共通鍵SymK #1を復号化し(ステップ701)、続いて、共通鍵SymK #1で登録フォーム要求を復号化し(ステップ702)、登録フォーム選択情報から証明書発行に必要な証明書名組を決定し、登録フォームを作成する(ステップ703)。この証明書名組の決定の方法としては、例えば、

(1) 登録フォーム選択情報に記述されているブランド名をキーにして、認証局の証明書名データベースから検索する

(2) 登録フォーム選択情報にブランド名だけでなく、必要な証明書名組まで含めておく
などがある。

【0062】そして、認証局10は、ステップ703で作成した登録フォームに対して、認証局10の署名鍵個人鍵PVCPSG(11512)で署名し(ステップ704)、ステップ704で作成した署名つき登録フォームに、認証局10の証明書CertPBCPSG(11513)をつけ、カード所有者のクライアント20へ送信する(ステップ705)。このように、前記証明書名データベースを基に、送信電子証明書で発行可能な他の証明書のリスト、または証明書の発行に必要な証明書組をカード所有者のクライアントに送信することにより、証明書発行にかかる手間を少なくすることができる。

【0063】次に、上述したステップ405を図8を用いて詳細に説明する。

【0064】ステップ405は、図8に示すように、まず、カード所有者のクライアント20が、受信した署名の証明書CertPBCPSGの妥当性を、SETと同様な手段により検証する(ステップ801)。

【0065】その検証の結果、妥当でなければ処理を中

断し、妥当であれば処理を続け（ステップ802）、カード所有者の署名鍵公開鍵PBCHSG'（21120）および秘密鍵PVCHSG'（21160）を生成し、記憶装置211に保存し（ステップ803）、受信した登録フォームに必要事項を記入してこれを登録事項とする（ステップ804）。

【0066】その後、カード所有者のクライアント20は、受信した証明書名組にしたがって、証明書データベース21140から証明書を検索し、証明書組を作成する（ステップ805）。

【0067】ここで、証明書組とは、1個以上の複数個の証明書を、例えばリスト構造のように、ひとつのまとまりにしたものである。

【0068】カード所有者は、その証明書組を構成している複数個の証明書からカード所有者の署名鍵公開鍵21120を取り出し、カード所有者署名鍵公開鍵リストPBCHSGL（21180）とする（ステップ806）。

【0069】その後、カード所有者のクライアント20は、共通鍵SymK #2（21172）、共通鍵SymK #3（21173）を生成して記憶装置211に保存し（ステップ807）、登録事項を含んだ証明書要求メッセージを作成する（ステップ808）。

【0070】カード所有者20は、証明書要求メッセージおよびカード所有者の署名鍵公開鍵PBCHSG'（21120）、共通鍵SymK #2（21172）に対して、カード所有者の署名鍵公開鍵PBCHSG''で署名をつける（ステップ809）。ここで、PBCHSG''はカード所有者署名鍵公開鍵リストPBCHSGL（21180）に含まれているいずれか1個の公開鍵である。このPBCHSG''の選び方は、例えば、PBCHSGLの先頭の公開鍵を選択するとよい。このステップ809で、PBCHSG''の代わりにPBCHSGを使用すると、不正な証明書を使用することができるため、PBCHSG''を使用することが必須である。なお、既存のSETでは、本人確認を口座番号などを利用して行っているためPBCHSGを使用しても構わない。登録する公開鍵PBCHSG'は、PBCHSG''と同一とすることもできる。

【0071】カード所有者のクライアント20は、ステップ809の結果を、共通鍵SymK #3（21173）で暗号化し（ステップ810）、続いて、証明書組と共通鍵SymK #3（21173）を、認証局の鍵交換鍵公開鍵PBCPEX（11521）で暗号化し（ステップ811）、ステップ810およびステップ811で作成したものを、認証局10へ送信する（ステップ812）。

【0072】次に、上述したステップ406を図9を用いて詳細に説明する。

【0073】ステップ406は、図9に示すように、まず、認証局10が、カード所有者のクライアント20から受信したメッセージに対して、認証局の鍵交換鍵個人鍵PVCPEX（11522）を使って、証明書組と共通鍵SymK

mK #3（21173）を復号化する（ステップ901）。

【0074】その後、認証局10は、図8に示したステップ810で暗号化された部分を共通鍵SymK #3（21173）で復号化し（ステップ902）、カード所有者の署名をカード所有者の署名鍵公開鍵PBCHSG''を使って検証し（ステップ903）、検証の結果、妥当でなければ処理を中断し、妥当であれば処理を続行する（ステップ904）。

【0075】次に、上述したステップ408を図10を用いて詳細に説明する。

【0076】ステップ407は、図10に示すように、まず、認証局10が、証明書組を分解し（ステップ1001）、各々の証明書を検証し、証明書値を計算する（ステップ1002）。

【0077】その後、認証局10は、証明書要求メッセージから発行する証明書の名前を取り出し、証明書名データベース11530からその証明書を発行するために必要な証明書名組11533を検索し（ステップ1003）、ステップ1001の証明書名組11533にステップ1002の証明書値を代入して、証明書組値を計算する（ステップ1004）。ここでの証明書値は、証明書が妥当であれば"t"、妥当でなければ"f"と言う値を取る。また、証明書名組とは、複数の証明書名CN1,...,CNnを論理演算子(∧、∨、¬)で結合したものである。

【0078】例えば、(C1∧C2)∨(¬C3)は、証明書名組であり、その証明書名組の値とは、それぞれの証明書の値を証明書名組の「証明書名」へ代入し、論理演算した結果の値である。計算（論理演算）には、以下の論理規則を用いる。

【0079】A, B, Cは、0個以上のt, fを∧, ∨, ¬で結合した式を表す。結合度は、¬, ∧, ∨の順で弱くなる。

【0080】(1) $t \wedge t \rightarrow t$

(2) $t \wedge f \rightarrow f$

(3) $f \wedge t \rightarrow f$

(4) $f \wedge f \rightarrow f$

(5) $t \vee t \rightarrow t$

(6) $t \vee f \rightarrow t$

(7) $f \vee t \rightarrow t$

(8) $f \vee f \rightarrow f$

(9) $\neg t \rightarrow f$

(10) $\neg f \rightarrow t$

(11) $A \wedge B \wedge C \rightarrow (A \wedge B) \wedge C$

(12) $A \vee B \vee C \rightarrow (A \vee B) \vee C$

その後、認証局10は、その他の条件を確認する。ここで、「その他の条件」とは、証明書の妥当性以外の条件であり、例えば、「ある友の会の会員である」、「年齢が35歳以上である」などのカード所有者本人を確認する

ものである。これらの条件を、認証局10は、オンラインあるいはオフラインで確認し、その結果、条件に合っていれば条件値を"t"とし、条件に合わなければ条件値を"f"とする(ステップ1005)。これにより、より確実に証明書の検証を行うことが可能になる。

【0081】その後、認証局10は、ステップ1004、ステップ1005の結果、証明書組値A条件値を前述の論理規則にしたがって計算し、その結果が"f"であれば処理を中断し、その結果が"t"であれば処理を続行する(ステップ1006)。

【0082】そして、証明書組値が"t"の場合、認証局10は、カード所有者に対して、請求されていた証明書を発行するため、カード所有者の署名鍵公開鍵PBCSG'(21120)に対して認証局10が署名した証明書CertPBCSG'(21140)を作成し(ステップ1007)、証明書要求応答メッセージを作成、署名して、共通鍵Sym #2(21172)で暗号化し(ステップ1008)、証明書CertPBCSG'(21140)、および、ステップ1008で作成した署名つき証明書要求応答メッセージを暗号化したものと、認証局10の証明書CertPBCPSG(11513)とを、カード所有者20に対して送信する(ステップ1009)。

【0083】次に、上述したステップ409を図11を用いて詳細に説明する。

【0084】ステップ409は、図11に示すように、まず、カード所有者のクライアント20が、認証局から受信した証明書CertPBCPSG(21113)の妥当性を、上述したように、SETと同様に検証する(ステップ1101)。

【0085】その検証の結果、妥当でなければ処理を中断し、妥当であれば処理を続け(ステップ1102)、共通鍵Sym #2(21172)を記憶装置211から取り出し、この共通鍵Sym #2(21172)で証明書応答メッセージを復号化し(ステップ1103)、認証局10の署名鍵公開鍵PBCPSG(11511)で署名を検証し(ステップ1104)、署名が確認されなければ処理を中断し、確認されれば処理を続行する(ステップ1105)。

【0086】そして、カード所有者のクライアント20は、発行された証明書CertPBCSG'(21140)を記憶装置211に保存する(ステップ1106)。

【0087】したがって、説明してきたように、ある認証局が既に発行した公開鍵の証明書とその証明書におけるカード所有者の公開鍵に対して、証明書で証明済の鍵でデジタル署名を施したものと発行を要求する証明書名の入力を受け、カード所有者のデジタル署名が妥当であるか否かを検証し、妥当であると検証できたときは、証明書と証明書名データベースとを照合し、カード所有者が要求した証明書が発行可能である場合には、送信された証明書の検証を行い、検証できた場合に、カード所有

者の公開鍵を認証した証明書を発行することにより、カード所有者の身元確認の根拠として、電子的に送付可能で信頼性のある既に取得した証明書をを用いることが可能になり、カード所有者から認証局へ口座番号を送ったり、認証局がその口座番号が正しいかどうかを銀行に確認したりする必要がなくなるので、低コストで証明書を発行することが可能になる。

【0088】また、プライバシーに関わる個人情報を送付する必要がなくなるため、全体のセキュリティ強度を高めることが可能になる。

【0089】なお、上述した証明書発行処理を行う証明書発行システムの各制御装置は、コンピュータで実行可能なプログラムで実現される場合もあり、そのときのプログラムは、フロッピーディスク、CD-ROM、マスクROM等の記憶媒体で一般ユーザに提供される。この場合、さらに、これら処理の他にGUIプログラム等の他のプログラムと組み合わせてユーザに提供することもある。

【0090】また、上述した記憶媒体で提供する代替手段として、インターネット等のネットワークを通じて有償で提供することもある。

【0091】以上、本発明者によってなされた発明を、前記実施形態に基づき具体的に説明したが、本発明は、前記実施形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。

【0092】

【発明の効果】本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば、下記のとおりである。

【0093】カード所有者の身元確認の根拠として、電子的に送付可能で信頼性のある既取得証明書をを用いることが可能になり、カード所有者から認証局へ口座番号を送ったり、認証局がその口座番号が正しいかどうかを銀行に確認したりする必要がなくなるので、低コストで証明書を発行することが可能になる。

【0094】また、プライバシーに関わる個人情報を送付する必要がなくなるため、全体のセキュリティ強度を高めることが可能になる。

【図面の簡単な説明】

【図1】本発明の実施形態にかかる電子証明書発行システムの構成を説明するためのブロック図である。

【図2】認証局の構成を詳細に説明するための図である。

【図3】カード所有者のクライアントを詳細に説明するための図である。

【図4】本実施形態の証明書発行システムの各制御装置における証明書発行処理の概要を説明するためのフローチャートである。

【図5】認証局が、カード所有者からの証明書要求メッ

セージに回答するメッセージを作成し、カード所有者へ送信する処理を示すフローチャートである。

【図6】カード所有者が、認証局から証明書要求応答メッセージを受け取って、認証局へ登録フォーム要求メッセージを送信する処理を示すフローチャートである。

【図7】認証局が登録フォームを生成し、カード所有者に送信する処理を示すフローチャートである。

【図8】カード所有者が登録フォームを記入し、証明書要求を認証局へ送信する処理を示すフローチャートである。

【図9】認証局がカード所有者の証明書組を検証する処理を示すフローチャートである。

【図10】認証局が、検証の結果に応じて証明書を発行し、カード所有者へ証明書を送信する処理を示すフロー

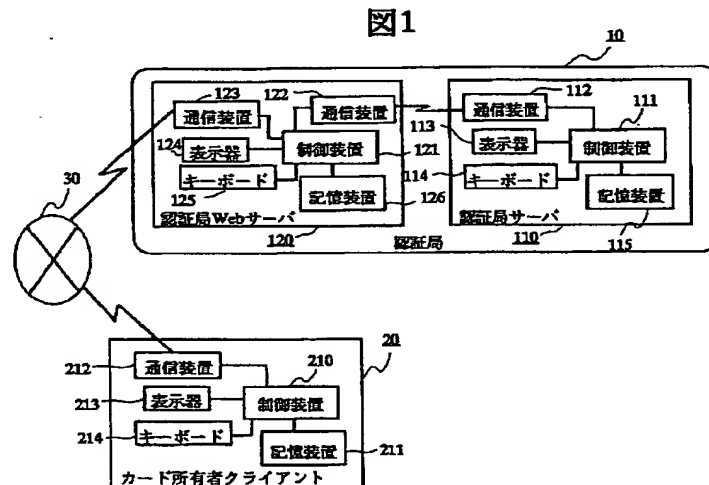
チャートである。

【図11】カード所有者が、認証局によって発行された証明書を検証し保存する処理を示すフローチャートである。

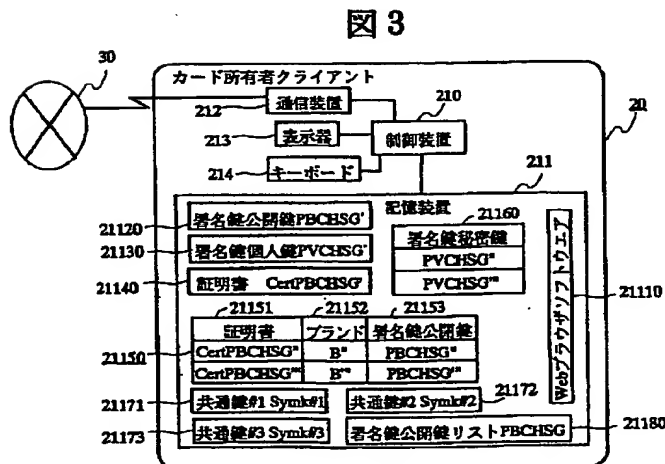
【符号の説明】

10…認証局、20…クライアント、30…インターネット、110…認証局サーバ、111…制御装置、112…通信装置、113…表示器、114…キーボード、115…記憶装置、120…認証局Webサーバ、121…制御装置、122…通信装置、123…通信装置、124…表示器、125…キーボード、126…記憶装置、210…制御装置、211…記憶装置、212…通信装置、213…表示器、214…キーボード。

【図1】

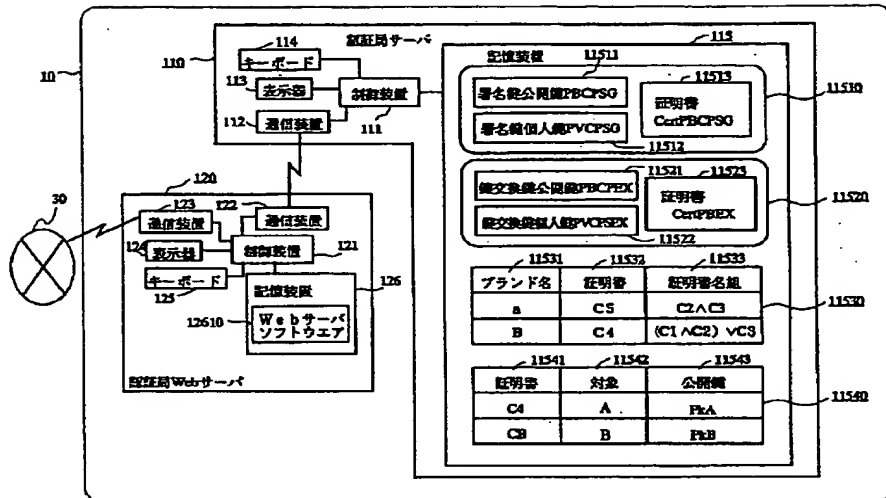


【図3】



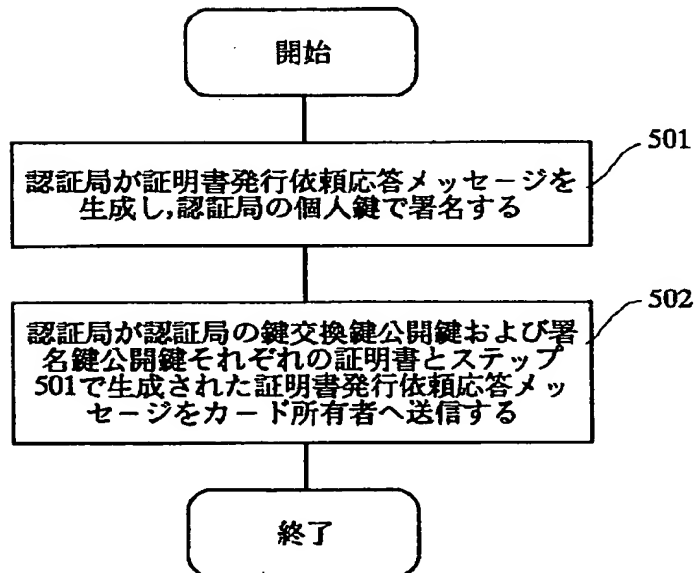
【図 2】

図 2

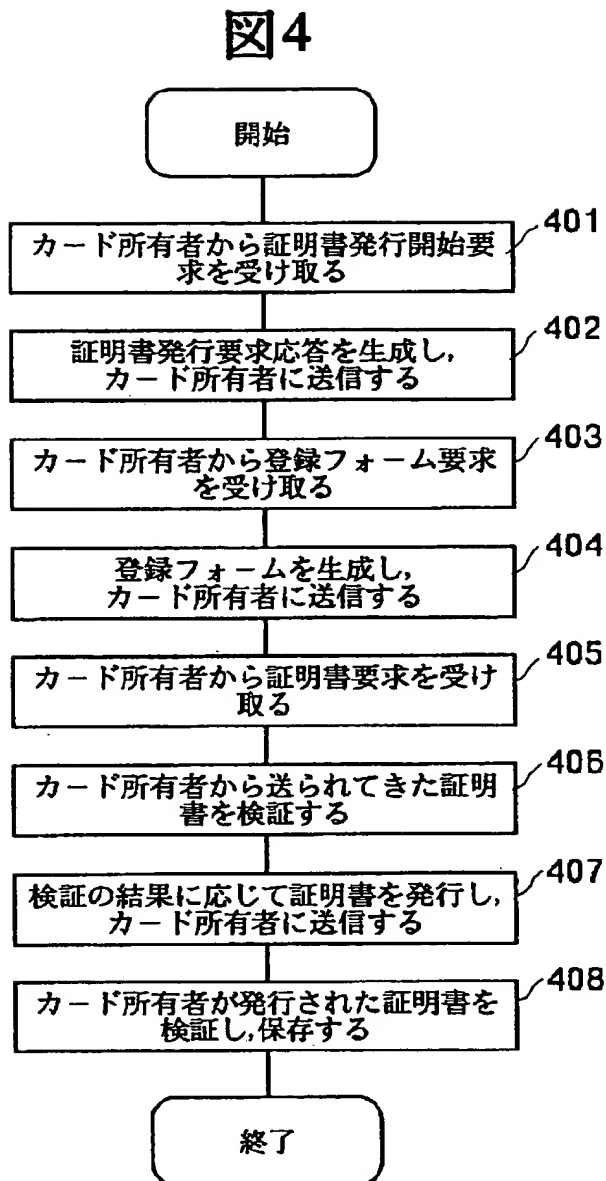


【図 5】

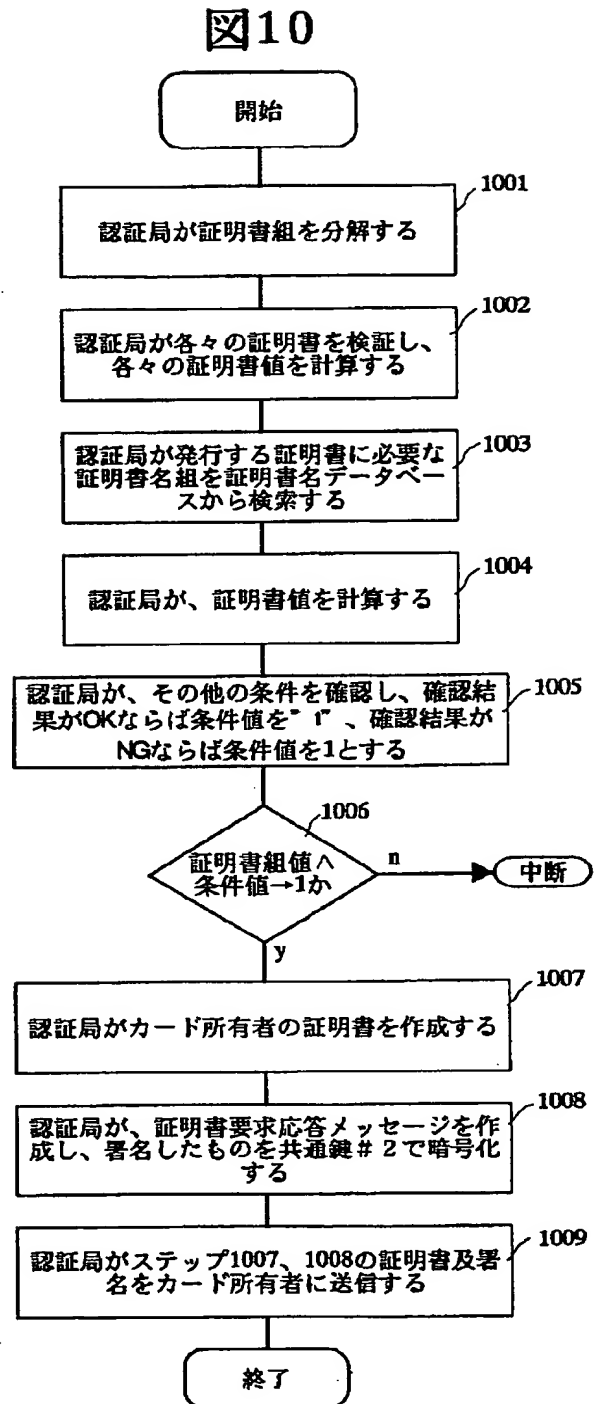
図 5



【図4】

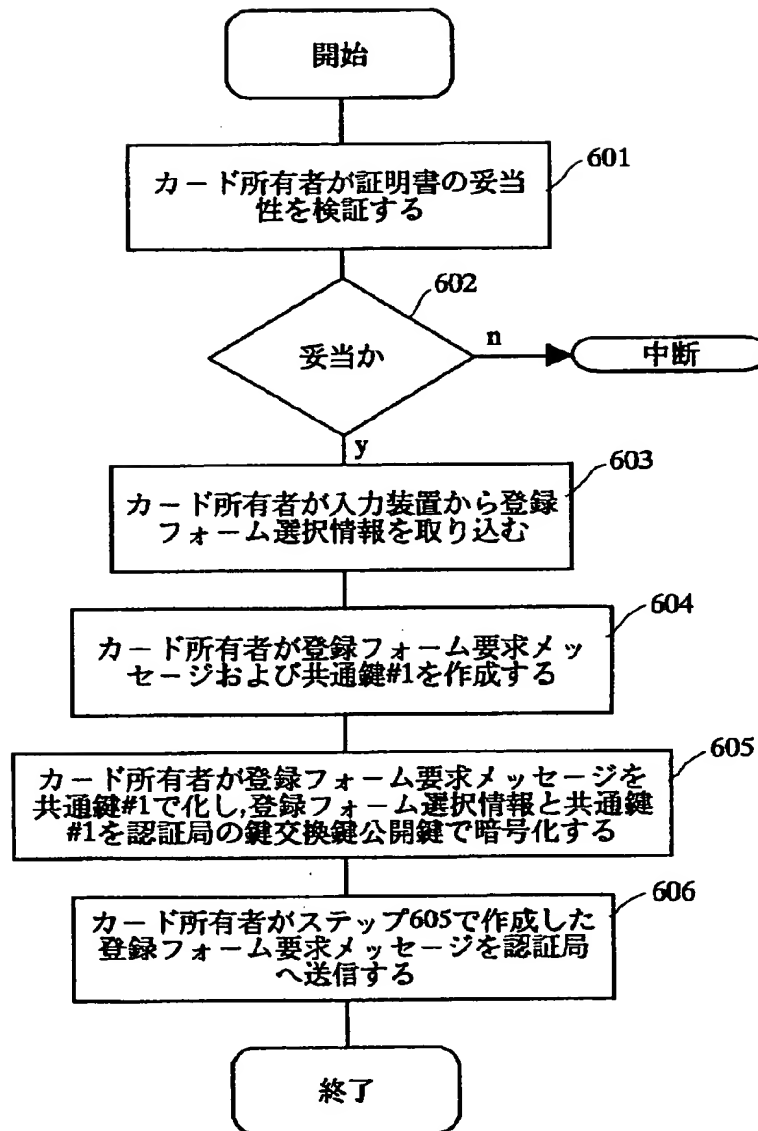


【図10】



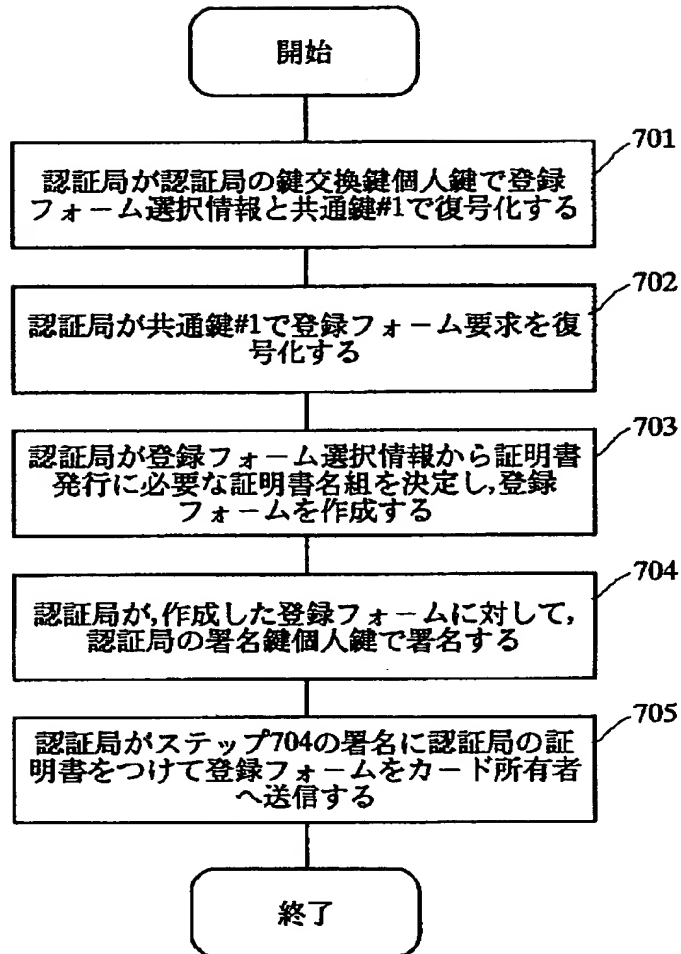
【図6】

図6



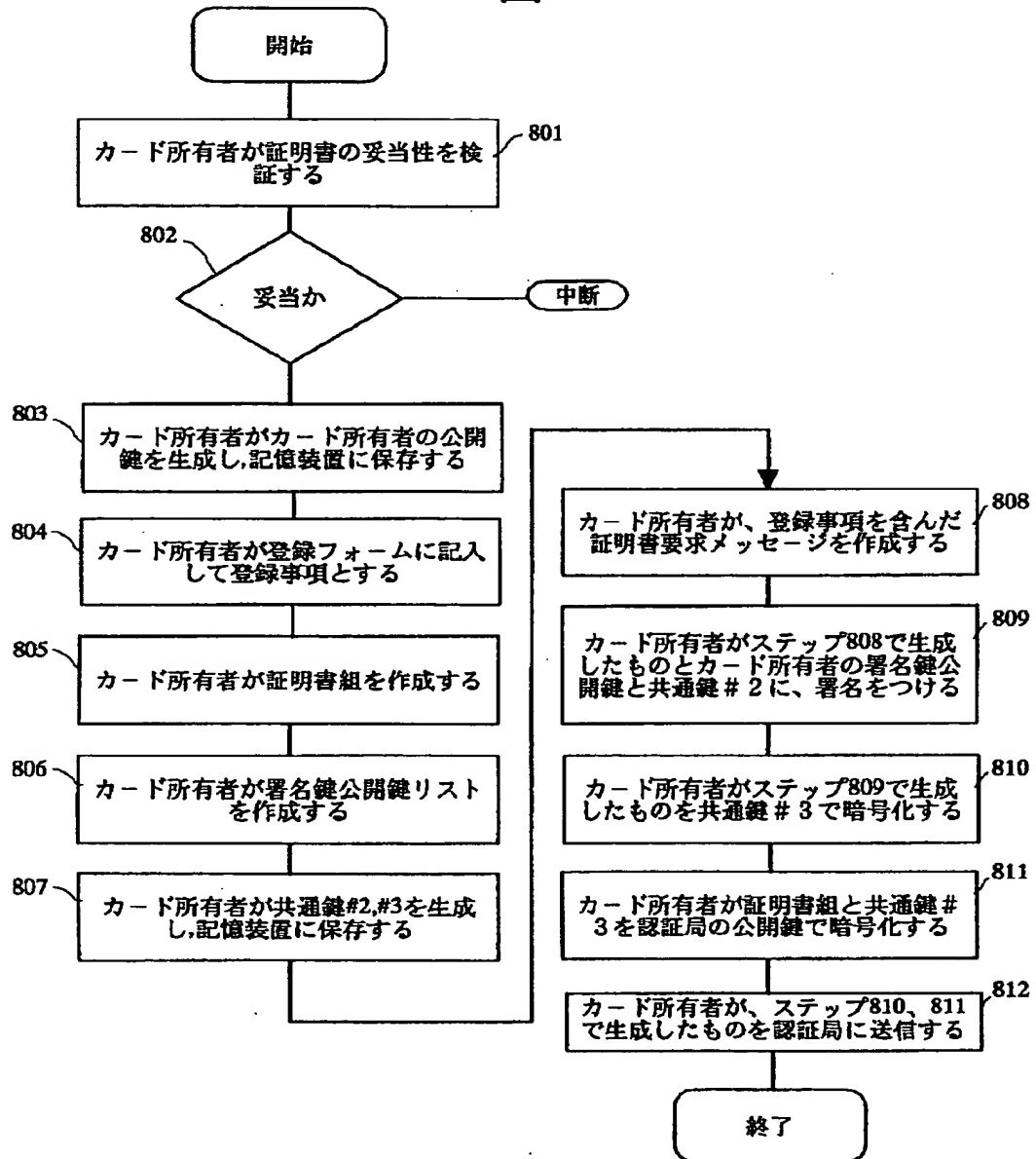
【図7】

図7



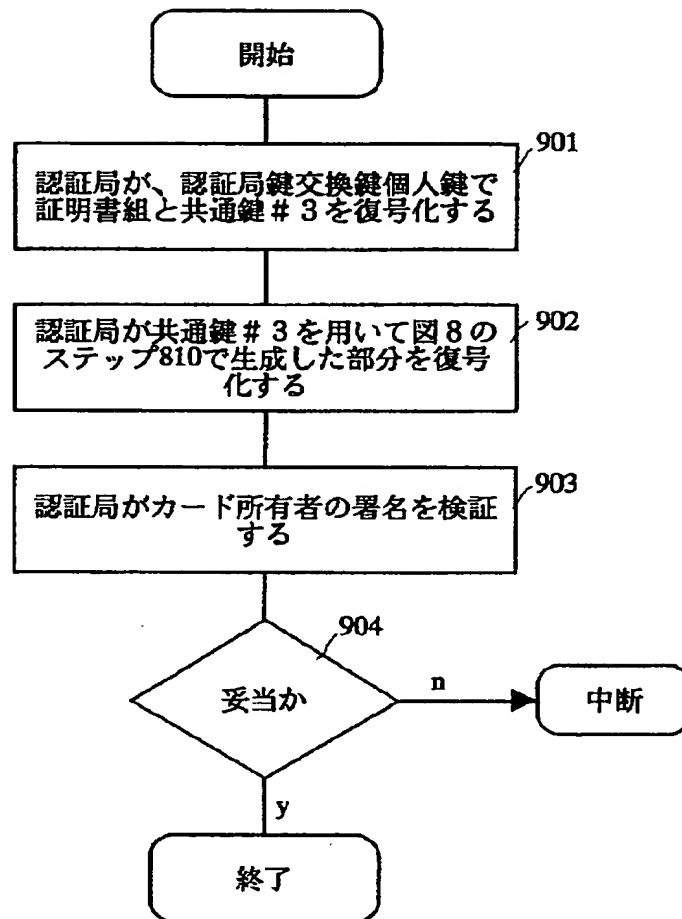
【図 8】

図 8



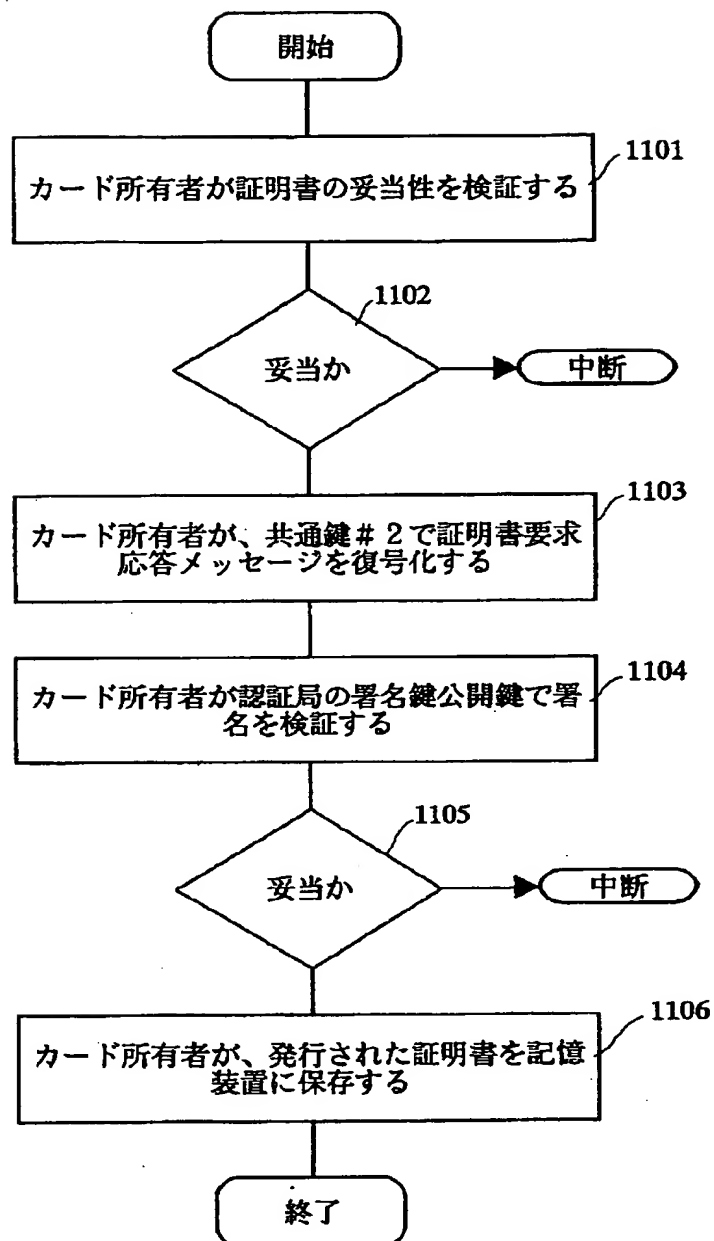
【図 9】

図 9



【図 11】

図 11



フロントページの続き

(72)発明者 川連 嘉晃
神奈川県横浜市都筑区加賀原二丁目2番
株式会社日立製作所ビジネスシステム開発
センタ内

(72)発明者 松永 和男
神奈川県横浜市戸塚区戸塚町5030番地 株
式会社日立製作所ソフトウェア開発本部内

(72)発明者 州崎 誠一
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内